

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-152713

(43)Date of publication of application : 23.05.2003

(51)Int.Cl.

H04L 9/32
G06F 15/00

(21)Application number : 2001-350006

(71)Applicant : CANON INC

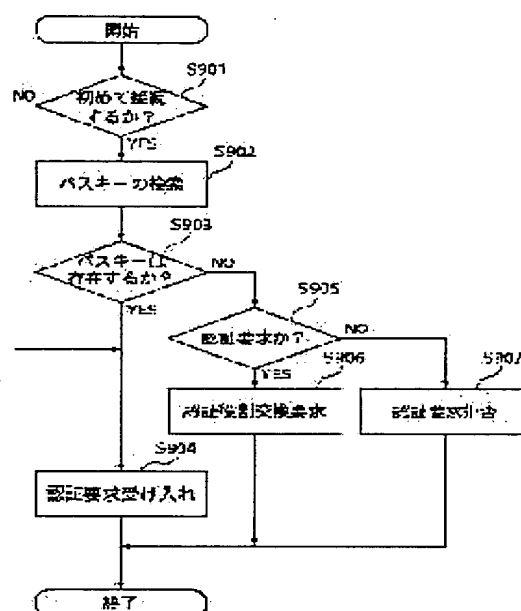
(22)Date of filing : 15.11.2001

(72)Inventor : FUJITA SHIGERU

(54) METHOD FOR AUTHENTICATING COMMUNICATION OPPOSITE PARTY, INFORMATION COMMUNICATION SYSTEM, AND CONTROL PROGRAM**(57)Abstract:**

PROBLEM TO BE SOLVED: To provide a method for authenticating communication opposite parties by which even information communication devices unable to receive authentication information required to authenticate the communication opposite party can conduct authentication processing.

SOLUTION: In the case that an information communication device acting like an authentication side receives its own password and an address and an information communication device acting like a side to be authenticated receives the password and the address of the information communication device acting like the authentication side to conduct the authentication processing, the information communication device acting like the authentication side registers in advance passwords and addresses of information communication devices to be communication opposite parties, and when the information communication device acting like the authentication side becomes an information communication device acting like the side to be authenticated, the information communication device acting like the authentication side becoming the information communication device acting like the side to be authenticated uses the password and the address having been stored in advance of an information communication device acting like the authentication side to conduct the authentication processing. Further, when the own device has no function of receiving a password and an address of an information communication device at the authentication side in spite of it that the own device becomes the side to be authenticated and stores no password nor address, the own device responds it to the information communication device acting like at present the authentication side that the own device changes the roll to act like the authentication side.

**LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

THIS PAGE LEFT BLANK

the examiner's decision of rejection or
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

THIS PAGE LEFT BLANK

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2003-152713

(P 2003-152713 A)

(43) 公開日 平成15年5月23日 (2003. 5. 23)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/32		G 0 6 F 15/00 3 3 0 C	5B085
G 0 6 F 15/00	3 3 0	H 0 4 L 9/00 6 7 3 A	5J104

審査請求 未請求 請求項の数 2 3 O L

(全 1 3 頁)

(21) 出願番号 特願2001-350006 (P2001-350006)

(22) 出願日 平成13年11月15日 (2001. 11. 15)

(71) 出願人 000001007

キャノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 藤田 茂

東京都大田区下丸子3丁目30番2号

キャノ
ン株式会社内

(74) 代理人 100081880

弁理士 渡部 敏彦

F ターム (参考) 5B085 AE04

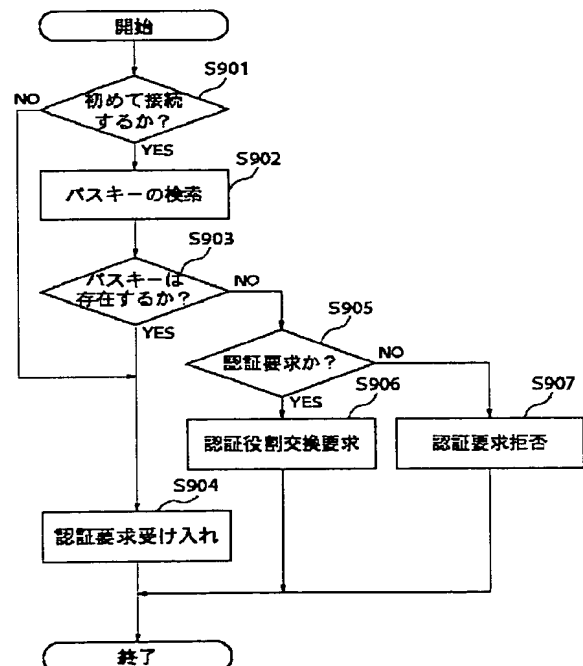
5J104 AA07 EA03 KA02

(54) 【発明の名称】 通信相手認証方法、情報通信システム、及び制御プログラム

(57) 【要約】

【課題】 通信相手を認証するのに必要な認証情報を入力できない情報通信装置同士でも認証処理を行えるようにする。

【解決手段】 認証側となる情報通信装置は自己のパスワードとアドレスを入力し、被認証側となる情報通信装置は認証側となる情報通信装置のパスワードとアドレスを入力することにより認証処理を行う場合に、通信相手となり得る情報通信装置のパスワードとアドレスを予め登録しておき、自装置が被認証側となった場合は、予め記憶しておいた認証側の情報通信装置のパスワードとアドレスを使用して認証処理を遂行する。また、自装置が被認証側となったにも拘わらず、自装置が該認証側の情報通信装置のパスワードとアドレスを入力する機能を持たず、かつパスワードとアドレス記憶していないときは、役割を交代して自装置が認証側になる旨の応答を現在認証側となっている情報通信装置に対して行う。



【特許請求の範囲】

【請求項 1】 通信を開始する際に通信相手となる情報通信装置を認証する通信相手認証方法であって、被認証側となる情報通信装置は、認証側となる情報通信装置の認証情報を該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておき、認証処理の際には、記憶しておいた認証情報を使用して認証手続きを行うことを特徴とする通信相手認証方法。

【請求項 2】 前記通信相手認証方法は、認証側となる情報通信装置は、自己の認証情報を入力し、被認証側となる情報通信装置は認証側となる情報通信装置の認証情報を入力することにより、認証処理を遂行することを特徴とする請求項 1 に記載の通信相手認証方法。

【請求項 3】 前記被認証側となる情報通信装置は、前記認証側となる情報通信装置から認証要求が発せられた場合に、自装置が該認証側となる情報通信装置の認証情報を入力する機能を持たず、かつ該認証情報を前記記憶媒体に記憶していないときは、自装置が認証側になる旨の応答を現在認証側となっている情報通信装置に対して行うことを特徴とする請求項 1 又は 2 に記載の通信相手認証方法。

【請求項 4】 前記認証情報は、パスワード情報とアドレス情報であることを特徴とする請求項 1 ～ 3 の何れかに記載の通信相手認証方法。

【請求項 5】 前記認証側となる情報通信装置と、被認証側となる情報通信装置は、前記認証情報の 1 つとして自装置のアドレス情報を予め記憶していることを特徴とする請求項 1 ～ 4 の何れかに記載の通信相手認証方法。

【請求項 6】 前記認証処理は、所定の規格の無線通信を行う場合に実行されることを特徴とする請求項 1 ～ 5 の何れかに記載の通信相手認証方法。

【請求項 7】 前記所定の規格の無線通信は、blue tooth 規格の無線通信であることを特徴とする請求項 6 に記載の通信相手認証方法。

【請求項 8】 前記記憶媒体は、前記被認証側となる情報通信装置に予め内蔵された記憶媒体であることを特徴とする請求項 1 ～ 7 の何れかに記載の通信相手認証方法。

【請求項 9】 前記被認証側となる情報通信装置は、該被認証側となる情報通信装置にケーブルで接続された情報通信装置から前記認証側となる情報通信装置の認証情報を取得して前記予め内蔵された記憶媒体に記憶することを特徴とする請求項 8 に記載の通信相手認証方法。

【請求項 10】 前記記憶媒体は、前記被認証側となる情報通信装置に着脱自在な記憶媒体であることを特徴とする請求項 1 ～ 7 の何れかに記載の通信相手認証方法。

【請求項 11】 前記被認証側となる情報通信装置は、前記記憶媒体に予め記憶しておいた認証側となる情報通信装置の認証情報を使用して認証処理を行って通信した場合は、当該認証側となる情報通信装置へのリンク情報

を記憶しておき、当該認証側となる情報通信装置から再度認証要求がなされた際には、該リンク情報を検索することにより該認証要求を受理することを特徴とする請求項 1 ～ 10 の何れかに記載の通信相手認証方法。

【請求項 12】 通信相手となる情報通信装置を認証した後に通信を開始する情報通信システムであって、被認証側となる情報通信装置は、認証側となる情報通信装置の認証情報を該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておき、認証処理の際には、記憶しておいた認証情報を使用して認証手続きを行うことを特徴とする情報通信システム。

【請求項 13】 前記認証処理は、認証側となる情報通信装置は、自己の認証情報を入力し、被認証側となる情報通信装置は認証側となる情報通信装置の認証情報を入力することにより、認証処理を遂行するものであることを特徴とする請求項 12 に記載の情報通信システム。

【請求項 14】 前記被認証側となる情報通信装置は、前記認証側となる情報通信装置から認証要求が発せられた場合に、自装置が該認証側となる情報通信装置の認証情報を入力する機能を持たず、かつ該認証情報を前記記憶媒体に記憶していないときは、自装置が認証側になる旨の応答を現在認証側となっている情報通信装置に対して行うことを特徴とする請求項 12 又は 13 に記載の情報通信システム。

【請求項 15】 前記認証情報は、パスワード情報とアドレス情報であることを特徴とする請求項 12 ～ 14 の何れかに記載の情報通信システム。

【請求項 16】 前記認証側となる情報通信装置と、被認証側となる情報通信装置は、前記認証情報の 1 つとして自装置のアドレス情報を予め記憶していることを特徴とする請求項 12 ～ 15 の何れかに記載の情報通信システム。

【請求項 17】 前記認証処理は、所定の規格の無線通信を行う場合に実行されることを特徴とする請求項 12 ～ 16 の何れかに記載の情報通信システム。

【請求項 18】 前記所定の規格の無線通信は、blue tooth 規格の無線通信であることを特徴とする請求項 17 に記載の情報通信システム。

【請求項 19】 前記記憶媒体は、前記被認証側となる情報通信装置に予め内蔵された記憶媒体であることを特徴とする請求項 12 ～ 18 の何れかに記載の情報通信システム。

【請求項 20】 前記被認証側となる情報通信装置は、該被認証側となる情報通信装置にケーブルで接続された情報通信装置から前記認証側となる情報通信装置の認証情報を取得して前記予め内蔵された記憶媒体に記憶することを特徴とする請求項 19 に記載の情報通信システム。

【請求項 21】 前記記憶媒体は、前記被認証側となる情報通信装置に着脱自在な記憶媒体であることを特徴と

する請求項 12～18 の何れかに記載の情報通信システム。

【請求項 22】 前記被認証側となる情報通信装置は、前記記憶媒体に予め記憶しておいた認証側となる情報通信装置の認証情報を使用して認証処理を行って通信した場合は、当該認証側となる情報通信装置へのリンク情報を記憶しておき、当該認証側となる情報通信装置から再度認証要求がなされた際には、該リンク情報を検索することにより該認証要求を受理することを特徴とする請求項 12～21 の何れかに記載の情報通信システム。

【請求項 23】 通信相手となる情報通信装置を認証した後に通信を開始する情報通信システムにおいて被認証側となる情報通信装置により実行される制御プログラムであって、
認証側となる情報通信装置から認証要求がなされた場合に、該認証要求を受けて被認証側となる情報通信装置は、該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておいた認証側となる情報通信装置の認証情報を読み出し、該読み出した認証情報を使用して認証手続きを行う内容を有することを特徴とする制御プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、情報通信機器間における通信相手の認証技術に関する。

【0002】

【従来の技術】 従来、情報機器同士が通信を行う際、最も簡便な場合は、通信相手が如何なる機器であっても接続・通信を許可していた。しかし、複数の機器を対象に通信を行いたい場合、接続相手機器を識別してアクセス権を管理し、セキュリティを確保するために、ユーザ ID とパスワードを用いて管理・運用する方法が広く用いられてきた。

【0003】 近年、普及の著しいインターネットにおいては、ユーザ ID とパスワードによるアクセス管理が広く一般に行われている。ユーザは、ネットワーク接続時にユーザ ID とパスワード情報を送信し、認証されると通信を開始できるようになる。

【0004】 サーバ・クライアントモデルのネットワークでは、サーバ側にユーザ ID とパスワードを記録・管理しておき、クライアントから接続要求が来た時に送られてくるユーザ ID とパスワード情報を照合し、適合していればアクセス権を付与し、通信を開始するよう構成されている。ユーザが初めて通信を行う時は、予めユーザ情報をサーバ側に設定しておくか、ゲストアカウントで接続した後、ユーザ ID、パスワードをクライアント端末側から送信し、サーバ側に設定するよう構成されている。

【0005】 また、近年、ネットワークの物理媒体として電波を用いる無線ネットワークが普及してきている。

無線ネットワークにおいても、サーバ・クライアントモデル・ネットワークは、上記と同様のアクセス権の管理が行われている。

【0006】 このようなアクセス権の管理機能が、Bluetooth に代表されるような近距離無線ネットワーク機器、特に携帯機器に実装される場合、使用される場所を選ばないので、今までに一度も接続したことのない機器同士が通信をする機会が増えることが予想される。また、無線通信なので、いつ、どの機器同士が接続しているのかがユーザには判り難く、通信していることに気付かない間にユーザの情報が盗まれる等の被害を防ぐためには、強固なセキュリティの実現が重要となる。

【0007】 Bluetooth 規格では、上記セキュリティの問題に対応するため、機器間の接続通信前に認証を行う方法が考慮されている。Bluetooth 規格におけるリンクレイヤーの機器認証の動作を以下に示す。

【0008】 機器認証は、1 対 1 の機器間で行われる。図 10 を参照しながら詳細を説明する。図 10 は、Bluetooth 機能を搭載した 2 つの端末 A と B の間での認証処理時のやりとりと各端末内部で実行される処理について時系列順に表したものである。図 10 の上部から下部へ向かって時間が経過するものとする。図 10 の左側の実線の左側が端末 A 内部を、右側の実線の右側が端末 B 内部を表している。図 10 の中央の実線と実線の間の破線矢印が、端末 A と端末 B 間の電波による情報通信を示している。

【0009】 通信接続時に端末 A、端末 B のどちらかが、通信相手を認証する認証側或いは被認証側として、認証プロセスを起動し、認証手続きの開始を要求する。ここでは、ユーザ A が端末 A をユーザ B が端末 B を操作するものとする。

【0010】 図 10 では端末 A が通信相手を認証する認証側、端末 B が通信相手として認証される被認証側となり、端末 A がステップ S501 で認証要求を端末 B へ送り、認証プロセスを起動する。端末 B はステップ S502 で認証受付応答を返し、認証手続きを開始する。ステップ S503 では、端末 A 内部で生成した乱数 1 (531) を端末 B へ送信する一方、端末 A 自身の持つ Bluetooth パスキー (以下パスキー) と呼ばれる文字列または数字列を端末 A のユーザ A に入力させる。

【0011】 パスキーとは、Bluetooth 対応端末が持つ機器固有のパスワード情報であり、今まで接続したことのない、言い換えると初めて接続する端末と認証手続きを行う際に使用される情報である。入力されたパスキー A (532) とパスキー A の長さであるパスキー A 長 (533) を演算アルゴリズム 1A (534) の入力として使用する。

【0012】 演算アルゴリズム 1A (534) は、初期化キー生成アルゴリズムであり、端末 A 内部で実行さ

10

20

30

40

50

れ、鍵情報である初期化キー 1 A (5 3 8) を生成する。乱数 1 (5 3 1) を受け取った端末 B 内部では、端末 A 同様、ユーザ B に端末 A のパスキー A を入力させ、入力されたパスキー A (5 3 5) とパスキー A の長さであるパスキー A 長 (5 3 6) を演算アルゴリズム 1 B (5 3 7) の入力として使用する。

【 0 0 1 3 】なお、端末 A に対してユーザ A が入力するパスキー A (5 3 2) と端末 B に対してユーザ B が入力するパスキー A (5 3 5) は同一であるべきものである。換言すれば、被認証側が認証側のパスキーを正しく

10 入力することを条件として、被認証側を認証側の通信相手として認証するのである。
【 0 0 1 4 】従って、パスキー A 長 (5 3 3) とパスキー A 長 (5 3 6) も同一となるべきものである。また、端末 B 内部で実行される演算アルゴリズム 1 B (5 3 7) と端末 A 内部で実行される演算アルゴリズム 1 A (5 3 4) も、同一のアルゴリズムである。端末 B でも端末 A と同様に初期化キー 1 B (5 3 9) が生成されるが、これも端末 A で生成される初期化キー 1 A (5 3 8) と同一となるべきものである。

【 0 0 1 5 】次に、端末 A は乱数 1 (5 3 1) とは異なる乱数 2 (5 4 0) を生成し、ステップ S 5 0 4 において端末 B へ送信する。また、上記乱数 2 (5 4 0) 、上記初期化キー 1 A (5 3 8) と被認証側である端末 B の Bluetooth Device Address (以下 BD_ADDR_B) (5 4 1) を演算アルゴリズム 2 A (5 4 2) の入力として使用し、演算結果 A (5 4 5) を得る。

【 0 0 1 6 】演算アルゴリズム 2 A (5 4 2) は、接続認証アルゴリズムであり、端末 A 内部で実行される。なお、BD_ADDR_B は各 Bluetooth 機器固有のアドレス番号であり、かつ認証手続き処理を開始する前段階、すなわちステップ S 5 0 1 を実行する前に、機器同士が接続を確立する際に交換する情報に含まれているので、この時点では既知の情報となっている。

【 0 0 1 7 】乱数 2 (5 4 0) を受け取った端末 B 内部では、端末 A 同様、乱数 2 (5 4 0) 、上記初期化キー 1 B (5 3 9) と端末 B の BD_ADDR_B (5 4 3) を演算アルゴリズム 2 B (5 4 4) の入力として使用し、演算結果 B (5 4 6) を得る。端末 B 内部で実行される演算アルゴリズム 2 B (5 4 4) と端末 A 内部で

40 実行される演算アルゴリズム 2 A (5 4 2) は、同一のアルゴリズムである。また、端末 A で使用する BD_ADDR_B (5 4 1) と、端末 B で使用する BD_ADDR_B (5 4 3) は、同一の情報である。
【 0 0 1 8 】次に、端末 B は、ステップ S 5 0 5 において、演算結果 B (5 4 6) を端末 A へ送信する。端末 A では、ステップ S 5 0 6 A において、端末 A 自身の内部で演算・生成した演算結果 A (5 4 5) と、端末 B 内部で演算・生成されて端末 B から送信された演算結果 B

(5 4 6) とを比較する。演算結果 A と演算結果 B の値が等しければ、認証は成功とし、値が異なると認証は失敗とする。認証が成功すると、端末 B を正当な通信相手として認証し、次の通信処理へと進む。また、認証に失敗した場合は、接続を切断して処理を終了する。

【 0 0 1 9 】なお、セキュリティレベルをより高めるため、認証成功後、端末 A と端末 B の認証役割を交換、すなわち、今度は端末 A が被認証側、端末 B が認証側となり、端末 B で生成する乱数と端末 B の持つパスキー B と

10 端末 A の BD_ADDR_A をパラメータとして、図 1 0 と同様の手続きで認証を行い、端末相互で認証処理を行うことも可能である。ただし、上記役割を交換して行う認証処理は、省略可能である。
【 0 0 2 0 】上述した認証動作は、通信を行う双方の端末共にユーザがパスキーを入力可能な場合であるが、Bluetooth を搭載した機器の中にはユーザがパスキーを入力することが困難であるか、又は入力できない機器も存在する。

【 0 0 2 1 】このような機器の場合、固定パスキーを予め機器内蔵のメモリに設定しておき、認証時に通信相手

20 端末のユーザに前記固定パスキーの入力を促し、自分のパスキーは前記固定パスキーを内蔵メモリから読み出して使用することによって、パスキー入力不能な機器のユーザがパスキーを入力しなくても良い方法が考慮されている。
【 0 0 2 2 】この例を図 1 1 に基づいて説明する。なお、図 1 1 の例では、端末 A がパスキー入力可能な端末、端末 C がパスキー入力不能な端末となっている。また、図 1 1 の表現方法は、図 1 0 と同様である。

30 【 0 0 2 3 】ステップ S 6 0 1 で、端末 A が認証側として認証要求を端末 C へ送り、認証プロセスを起動する。端末 C においてはユーザ C がパスキーを入力することができないので、ステップ S 6 0 2 で、被認証側として認証プロセスを実行することを拒否し、端末 A に対して認証側と被認証側との役割を交換し、端末 C が認証側となることを要求する認証役割交換要求を送信する。

【 0 0 2 4 】端末 A においてはユーザ A がパスキーを入力することができるので、端末 C からの認証役割交換要求を受け付けて、ステップ S 6 0 3 で認証受付応答を返し、認証手続きを開始する。このとき、図 1 1 に示したように、端末 A は被認証側、端末 C は認証側に役割が交換される。この後は、図 1 0 のステップ S 5 0 3 以降の処理と同等の処理が、端末 A が被認証側、端末 C が認証側として行われる。ただし、この場合、端末 C は、予め端末 C 内に設定されている、図示しない固定パスキー C を演算アルゴリズム 1 C への入力に使用する点が異なる。

【 0 0 2 5 】次に、通信を行う双方の端末共にユーザがパスキーを入力できない機器、すなわち固定パスキーを持つ機器同士の場合の認証手続き例を、図 1 2 に基づい

て説明する。図12の表現方法は図10と同様である。

【0026】ステップS701で、端末Cが認証側として認証要求を端末Dへ送り、認証プロセスを起動する。端末Dは、パスキーを入力することができないので、ステップS702で、被認証側として認証プロセスを実行することを拒否し、端末Cに対して認証側と被認証側との役割を交換し端末Cが認証側となることを要求する認証役割交換要求を送信する。

【0027】しかし、端末Cでもユーザがパスキーを入力することができないので、認証役割交換要求を受け付けることができず、ステップS703で、役割交換拒否応答を端末Dへ返す。この時点で、端末C、端末Dが共に被認証側になることを拒否し合ったため、認証手続きを開始することができず、通信を切断するよう動作していた。

【0028】

【発明が解決しようとする課題】上述したように、従来のBluetooth規格における機器接続時の認証方法では、ユーザがパスキーを入力できない機器同士を認証処理実行後に接続しようとする、どちらの機器も機器内に記憶してある固定パスキーを認証に使用し、被認証側ではなく認証側となって認証手続きを行おうとするので、認証手続きの役割分担が成立せず、結果として接続・通信することができないという欠点があった。従って、ユーザにとっては機器の使い勝手が非常に悪くなっていた。

【0029】本発明は、このような従来技術の問題に鑑みてなされたもので、その課題は、通信相手を認証するのに必要な認証情報を入力できない情報通信装置同士でも認証処理を行えるようにすることにある。

【0030】

【課題を解決するための手段】上記課題を解決するため、本発明は、通信を開始する際に通信相手となる情報通信装置を認証する通信相手認証方法であって、被認証側となる情報通信装置は、認証側となる情報通信装置の認証情報を該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておき、認証処理の際には、記憶しておいた認証情報を使用して認証手続きを行うように構成されている。

【0031】また、本発明は、通信相手となる情報通信装置を認証した後に通信を開始する情報通信システムであって、被認証側となる情報通信装置は、認証側となる情報通信装置の認証情報を該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておき、認証処理の際には、記憶しておいた認証情報を使用して認証手続きを行うように構成されている。

【0032】また、本発明は、通信相手となる情報通信装置を認証した後に通信を開始する情報通信システムにおいて被認証側となる情報通信装置により実行される制御プログラムであって、認証側となる情報通信装置から

認証要求がなされた場合に、該認証要求を受けて被認証側となる情報通信装置は、該被認証側となる情報通信装置が直接読み取り可能な記憶媒体に予め記憶しておいた認証側となる情報通信装置の認証情報を読み出し、該読み出した認証情報を使用して認証手続きを行う内容を有している。

【0033】

【発明の実施の形態】以下、本発明の実施の形態を、図面に基づいて詳細に説明する。

10 【0034】〔第1の実施形態〕図1は、本発明の第1実施形態に係るBluetooth機能を搭載したデジタルカメラのブロック図、図2は、Bluetooth機能を搭載したプリンタのブロック図である。本実施形態に係るプリンタは、パスキーの入力手段を持たない機器であり、固定パスキーを本体内に記憶している。本実施形態に係るデジタルカメラは、外部機器から本デジタルカメラ内のメモリに予め書き込んでおいた接続通信相手（プリンタ）のBD_ADDRとパスキーを読み出して、認証処理時に使用するように構成されている。

20 【0035】図1に示すデジタルカメラ100は、CPU101、ROM102、RAM103、不揮発性メモリ104、ワイヤレス通信回路部105、アンテナ106、外部機器接続コネクタ107、インタフェース回路部108、撮像部109、操作部110、表示部111、及び2次記憶部112を有しており、図示するように、内部バス113によって相互に接続されている。また、デジタルカメラ100は、電源回路部114を備え、前記各ブロックに電源ライン115によって電源を供給する。

30 【0036】CPU101は、ROM102に格納されているプログラムに従って動作し、デジタルカメラの各種動作を制御する。ROM102はデジタルカメラの制御手順（図4、5、7、10に対応する制御プログラムを含む）等を予め格納した不揮発性メモリである。RAM103は撮像部109から出力されるデジタル画像データの一時的なバッファリング、2次記憶部112へ書き込むデータや、2次記憶部から読み出したデータの一次的な記憶、CPU101の演算等に使用するワークエリア、ワイヤレス通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。

40 【0037】不揮発性メモリ104は、書き換え可能であり、機器の各種設定やBluetooth通信に使用する通信相手BD_ADDR、以前接続したBluetooth機器との通信に使用するリンクキー情報を記憶・保存する。ワイヤレス通信回路部105は、ワイヤレス通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するFIFOメモリ、自身のBD_ADDR_D、自身のパスキーDを記憶している不揮発性メモリ等から構成され、アンテナ106が接続され

ている。

【0038】外部機器接続コネクタ107は、外部機器とデジタルカメラ100を接続するコネクタである。インタフェース回路部108は、外部機器接続コネクタ107を介して接続された外部機器との間でデータ通信を行う機能を備えている。CPU101の制御に従い、外部機器へのデータの送信及び外部機器からのデータの受信を行う。

【0039】撮像部109は、入射する光を結像するレンズ、結像した光を電気信号へ変換する光電変換器（CCDやCMOSセンサ等）、光電変換器から出力されるアナログ電気信号をデジタル電気信号へ変換するADコンバータ（アナログ-デジタル変換器）等から成る。操作部110は、図示しない撮影を指示するリリースボタン、デジタルカメラ100の動作モードを選択するモード選択ダイヤル、メニュー項目を呼び出すメニューボタン、メニュー項目を選択・指示する十字カーソルボタン等のボタン、ダイヤル、スイッチで構成され、これらボタン、ダイヤル、スイッチの状態及び状態変化を電気信号として出力する。

【0040】表示部111は、液晶表示装置等で構成され、デジタルカメラ100の動作状態や撮影した画像データを表示する。2次記憶部112は撮影したデジタル画像データ等を格納する。電源回路部114はバッテリー、DC/DCコンバータ等で構成され、前述した各ブロックへ電源を供給する。

【0041】図2に示すプリンタ200は、CPU201、ROM202、RAM203、不揮発性メモリ204、ワイヤレス通信回路部205、アンテナ206、外部機器接続コネクタ207、インタフェース回路部208、印刷部209、操作部210、表示部211を有しており、図示するように内部バス212によって相互に接続されている。また、プリンタ200は電源回路部213を備え、前記各ブロックに電源ライン214によって電源を供給する。

【0042】CPU201は、ROM202に格納されているプログラムに従って動作し、プリンタの各種動作を制御する。ROM202はプリンタの制御手順（図4、5、7、10に対応する制御プログラムを含む）、フォントデータ等を予め格納した不揮発性メモリである。RAM203は外部機器から送信される印刷用データの一時的なバッファリング、印刷部へ送るデータへの変換作業用のワークエリア、CPU101の演算等に使用するワークエリア、ワイヤレス通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。

【0043】不揮発性メモリ204は、書き換え可能であり、機器の各種設定やBluetooth通信に使用する通信相手BD_ADDR、以前接続したBluetooth機器との通信に使用するリンクキー情報等を記

憶・保存する。ワイヤレス通信回路部205は、ワイヤレス通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するFIFOメモリ、自身のBD_ADDR_P、自身のバスキーPを記憶している不揮発性メモリ等から構成され、アンテナ206が接続されている。

【0044】外部機器接続コネクタ207は、外部機器とプリンタ200を接続するコネクタである。インタフェース回路部208は、外部機器接続コネクタ207を介して接続された外部機器との間でデータ通信を行う機能を備えている。CPU201の制御に従い、外部機器へのデータの送信及び外部機器からのデータの受信を行う。

【0045】印刷部209は印刷データを紙へ印刷するための印刷ヘッド、印刷ヘッド駆動モータ、紙搬送ローラ、紙搬送ギア駆動モータ、ギア等からなるプリントエンジン部である。操作部210は、図示しないプリンタの電源ON・OFFを指示する電源ボタン、リセットボタン等で構成され、これらボタン等の状態及び状態変化を電気信号として出力する。表示部211はLEDランプ等で構成され、プリンタ200の動作状態等を示す。電源回路部213はAC/DCコンバータ、DC/DCコンバータ等で構成され、前述した各ブロックへ電源を供給する。

【0046】第1の実施形態に係るデジタルカメラ100は、バスキー入力機能の無い機器（プリンタ）との間で認証処理を行うために、以下の設定が行われる。すなわち、図1に示すデジタルカメラ100の外部機器接続コネクタ107にパーソナルコンピュータをケーブルで接続し、予め調べておいたプリンタ200のBluetoothアドレス（BD_ADDR_P）とプリンタ200のバスキー情報（バスキーP）をリスト情報として、デジタルカメラ100の2次記憶部112の所定のエリアに書き込んでおく。

【0047】図3に、2次記憶部112内に格納されているバスキーリスト（1201）の例を示す。BD_ADDRとバスキーがペアとして格納されている。図3では[BD_ADDR_P（1202）、バスキーP（1203）]、[BD_ADDR_R（1204）、バスキーR（1205）]の2つのペアを持っている。ここでは2つのペアのバスキーリストを例示したが、ペアの個数に特に制限はない。

【0048】次に、デジタルカメラ100とプリンタ200の間で行うBluetooth通信の認証処理を、図面に基いて詳細に説明する。

【0049】図4は、プリンタ200が認証側、デジタルカメラ100が被認証側として認証手続きを行う場合の認証処理を示した図である。

【0050】プリンタ200がデジタルカメラ100に対して認証手続きを要求する（ステップS801）。プ

10

20

30

40

50

リント 200 からの認証要求を受け取ったデジタルカメラ 100 は、バスキー検索処理 (831) を実行する。バスキー検索処理 (831) の結果、プリント 200 の BD_ADDR_P、バスキー P が存在する場合、認証要求受付応答を、存在しない場合被認証側としての認証要求は受け付けず、プリント 200 に対して認証側と被認証側との役割を交換し、デジタルカメラ 100 が認証側となることを要求する認証役割交換要求を応答として送信する (ステップ S802)。

【0051】次に、図 4 に示したバスキー検索処理 (831) の詳細を、図 5 に基づいて説明する。なお、図 5 は、処理内容を一般化して示しているが、ここでは、今までの説明で用いた例に沿って説明する。

【0052】まず、認証要求を送信してきたプリント 200 が今回初めて接続する相手かどうかを判断する (ステップ S901)。具体的には、デジタルカメラ 100 の不揮発性メモリ 104 中に記憶されている機器接続リストの中に、プリント 200 の BD_ADDR_P に合致する BD_ADDR と、接続に必要なリンクキー P がリストアップされているかどうかを検索する。リストアップされていなければ、初めて接続する機器であるので

ステップ S902 へ進み、リストアップされていれば、ステップ S904 へ進む。

【0053】図 6 に機器接続リストの例を示す。BD_ADDR と前回認証接続時に生成した LINK KEY をペアとしたリスト (1101) として格納されている。図 6 には、[BD_ADDR_A (1102)、KEY_A (1103)]、[BD_ADDR_F (1104)、KEY_F (1105)]、[BD_ADDR_Z (1106)、KEY_Z (1107)] の 3 つのペアが記憶されており、ステップ S901 において、この機器接続リスト 1101 の中からプリント 200 の BD_ADDR である BD_ADDR_P を検索し、有るか否かを判定する。図 6 の機器接続リスト 1101 には、BD_ADDR_P が登録されていないので、プリント 200 は初めて接続する機器と判断され、ステップ S902 へ進むことになる。

【0054】次に、デジタルカメラ 100 の 2 次記憶部 112 に格納されたバスキーリスト 1201 の中に、プリント 200 の BD_ADDR_P とバスキー P がリストアップされているかどうかを検索する (ステップ S902)。そして、プリント 200 の BD_ADDR_P (1202) に対応するバスキー P (1203) がリストアップされているかどうかを判定する (ステップ S903)。バスキー P が存在すればステップ S904 へ進み、存在しなければステップ S905 へ進む。

【0055】ステップ S904 では、プリント 200 へ返す応答として、認証要求受け入れを選択する。ステップ S905 では、バスキー検索処理 831 を起動する要因が、認証要求か否かを判定する。その結果、認証要

求であった場合はステップ S906 へ進み、認証役割交換要求であった場合はステップ S907 へ進む。

【0056】ステップ S906 では、プリント 200 へ返す応答として認証役割交換要求を選択し、ステップ S907 では、プリント 200 へ返す応答として認証要求拒否を選択する。ステップ S904、906、907 の何れかの処理を行った後、本バスキー検索処理 (831) を終了する。

【0057】次に、図 4 とは逆に、プリント 200 が被認証側、デジタルカメラ 100 が認証側となって認証手続きを行う場合の認証処理を、図 7 に基づいて説明する。

【0058】ここでは、図 4 のように、プリント 200 がデジタルカメラ 100 に対して認証手続きを要求するのではなく、デジタルカメラ 100 が認証側となってプリント 200 に対して認証手続きを要求する (ステップ S1001)。デジタルカメラ 100 からの認証要求を受け取ったプリント 200 は、バスキー入力手段を持たないため、認証要求を拒否し、デジタルカメラ 100 に対して認証役割交換要求を送信する (ステップ S1002)。

【0059】プリント 200 からの認証役割交換要求を受け取ったデジタルカメラ 100 は、バスキー検索処理 (1031) を実行する。ここで行うバスキー検索処理 (1031) は、図 4 (図 5) に示したバスキー検索処理 (831) と同じである。バスキー検索処理 (1031) の結果、プリント 200 の BD_ADDR_P、バスキー P が存在する場合は、認証要求受付応答を、存在しない場合は、被認証側としての認証要求は受け付けず、プリント 200 に認証要求拒否応答を送信する (ステップ S1003)。

【0060】上述したように、第 1 の実施形態によれば、ユーザがバスキーを入力できないか、或いはバスキーの入力が困難な端末同士が通信開始時に認証処理を行う場合、従来は、認証手続きを実行できなかったが、本実施形態によれば、どちらか一方の端末 (本実施形態においてはデジタルカメラ 100) が、外部機器によって予め本体内のメモリに設定された通信相手端末の BD_ADDR とバスキー (本実施の形態においてはプリント 200 の BD_ADDR_P とバスキー P) を読み出して使用することにより、認証処理を行うことができる。従って、セキュリティを確保した状態で接続通信することが可能となるという効果がある。

【0061】なお、デジタルカメラ 100 に認証要求を送信してきたプリント 200 の BD_ADDR_P 或いはバスキー P が設定されていないと、デジタルカメラ 100 は従来と同様、認証要求を受け入れないので、未知の機器から勝手に接続されてしまうといった危険を排除することができる。

【0062】さらに、予め記憶しておいたアドレスとバ

10

20

30

40

50

スキーを認証処理に利用するので、これらを通信開始時に入力する手間が省けると共に、迅速に認証処理を完了して通信を開始することが可能となる。また、アドレスとバスキーを入力する必要がなくなるので、例えば、本来、入力機能と通信機能を持たない種類の電子機器にも通信機能を搭載するだけで本情報通信システムを適用可能となるなど、本情報通信システムを利用し得る情報通信装置の種類を増やすことができ、利便性を向上させることが可能となる。

【0063】〔第2の実施形態〕図8は、本発明の第2実施形態に係るBluetooth機能を搭載したデジタルカメラのブロック図、図9は、Bluetooth機能を搭載したプリンタのブロック図である。第2の実施形態におけるプリンタは、バスキーの入力手段を持たない機器であり、固定バスキーを本体内に記憶している。第2の実施形態におけるデジタルカメラは、外部機器によって予め接続通信相手のBD_ADDRとバスキーを書き込んでおいたメモリカードを装着し、認証処理時にメモリカードからバスキーを読み出して使用するものである。

【0064】図8に示すデジタルカメラ300は、CPU301、ROM302、RAM303、不揮発性メモリ304、ワイヤレス通信回路部305、アンテナ306、撮像部307、操作部308、表示部309、及びメモリカード・インタフェース回路部310を有しており、メモリカード314を前記メモリカード・インタフェース回路部310に装着することが可能である。各ブロックは、図示するように内部バス311によって相互に接続されている。また、デジタルカメラ300は電源回路部312を備え、前記各ブロックに電源ライン313によって電源を供給する。

【0065】CPU301は、ROM302に格納されているプログラムに従って動作し、デジタルカメラの各種動作を制御する。ROM302は、デジタルカメラの制御手順（図4、5、7、10に対応する制御プログラムを含む）等を予め格納した不揮発性メモリである。RAM303は、撮像部307から出力されるデジタル画像データの一時的なバッファリング、本体に装着したメモリカード314へ書き込むデータや、メモリカード314から読み出したデータの一時的な記憶、CPU301の演算等に使用するワークエリア、ワイヤレス通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。

【0066】不揮発性メモリ304は、書き換え可能であり、機器の各種設定やBluetooth通信に使用する通信相手のBD_ADDR、以前接続したBluetooth機器との通信に使用するリンクキー情報等を記憶・保存する。ワイヤレス通信回路部305は、ワイヤレス通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するFIFOメモリ、自身のBD

__ADDR__D、自身のバスキーDを記憶している不揮発性メモリ等から構成され、アンテナ306が接続されている。

【0067】撮像部307は、入射する光を結像するレンズ、結像した光を電気信号へ変換する光電変換器、光電変換器から出力されるアナログ電気信号をデジタル電気信号へ変換するADコンバータ等から成る。操作部308は、図示しない撮影を指示するリリースボタン、デジタルカメラ300の動作モードを選択するモード選択ダイヤル、メニュー項目を呼び出すメニューボタン、メニュー項目を選択・指示する十字カーソルボタン等のボタン、ダイヤル、スイッチで構成され、これらボタン、ダイヤル、スイッチの状態及び状態変化を電気信号として出力する。

【0068】表示部309は、液晶表示装置等で構成され、デジタルカメラ300の動作状態や撮影した画像データを表示する。メモリカード・インタフェース回路部310は、装着されたメモリカード314との間でデータの読み出し、書き込み、カード装着の有無の検出等を行う機能を備えている。電源回路部312は、バッテリー、DC/DCコンバータ等で構成され、前述した各ブロックへ電源を供給する。

【0069】図9に示すプリンタ400は、CPU401、ROM402、RAM403、不揮発性メモリ404、ワイヤレス通信回路部405、アンテナ406、外部機器接続コネクタ407、インタフェース回路部408、印刷部409、操作部410、表示部411、メモリカード・インタフェース回路部412、及びメモリカード413を有しており、図示したように、内部バス414によって相互に接続されている。また、プリンタ400は、電源回路部415を備え、前記各ブロックに電源ライン416によって電源を供給する。

【0070】CPU401は、ROM402に格納されているプログラムに従って動作し、プリンタの各種動作を制御する。ROM402はプリンタの制御手順（図4、5、7、10に対応する制御プログラムを含む）、フォントデータ等を予め格納した不揮発性メモリである。RAM403は、外部機器から送信される印刷用データの一時的なバッファリング、印刷部へ送るデータへの変換作業用のワークエリア、CPU401の演算等に使用するワークエリア、ワイヤレス通信回路部から送受信される通信データ、各種設定等を一時的に格納するエリアとして使用される。

【0071】不揮発性メモリ404は、書き換え可能であり、機器の各種設定やBluetooth通信に使用する通信相手BD_ADDR、以前接続したBluetooth機器との通信に使用するリンクキー情報等を記憶・保存する。ワイヤレス通信回路部405は、ワイヤレス通信に必要な高周波回路部、符号化・複合化回路部、無線通信時に使用するFIFOメモリ、自身のBD

__ADDR__P、自身のバスキーPを記憶している不揮発性メモリ等から構成され、アンテナ406が接続されている。

【0072】外部機器接続コネクタ407は、外部機器とプリンタ400を接続するコネクタである。インタフェース回路部408は、外部機器接続コネクタ407を介して接続された外部機器との間でデータ通信を行う機能を備えている。CPU401の制御に従い、外部機器へのデータの送信及び外部機器からのデータの受信を行う。

【0073】印刷部409は、印刷データを紙へ印刷するための印刷ヘッド、印刷ヘッド駆動モータ、紙搬送ローラ、紙搬送ギア駆動モータ、ギア等からなるプリントエンジン部である。操作部410は、図示しないプリンタの電源ON・OFFを指示する電源ボタン、リセットボタン等で構成され、これらボタン等の状態及び状態変化を電気信号として出力する。表示部411はLEDランプ等で構成され、プリンタ400の動作状態等を示す。メモリカード・インタフェース回路部412は、装着されたメモリカード413との間でデータの読み出し、書き込み、カード装着の有無の検出等を行う機能を備えている。電源回路部415は、AC/DCコンバータ、DC/DCコンバータ等で構成され、前述した各ブロックへ電源を供給する。

【0074】第2の実施形態に係るデジタルカメラ300においても、第1の実施形態に係るデジタルカメラ100と同様に、バスキー入力機能の無い機器（プリンタ）との間で認証処理を行うために、以下の設定が行われる。すなわち、図8に示すデジタルカメラ300に装着可能なメモリカード314を、パーソナルコンピュータ等の外部機器のメモリカードスロットへ装着し、予め調べておいたプリンタ400のBluetoothアドレス(BD__ADDR__P)と、プリンタ400のバスキー情報(バスキーP)を、メモリカード314の所定のエリアに書き込んでおく。

【0075】そして、通信を行う場合は、このメモリカード314をデジタルカメラ300に装着しておく。なお、メモリカード314内に設定されているBD__ADDRとバスキーリストは、第1の実施形態におけるデジタルカメラ100内蔵の不揮発性メモリ104内のバスキーリスト1201(図3参照)と同様のものである。

【0076】第2の実施形態における認証処理は、第1の実施形態と同様なので説明を省略する。ただし、第1の実施形態においては、デジタルカメラがプリンタのBD__ADDRとバスキーをデジタルカメラの2次記憶部から読み出したが、第2の実施形態においては、デジタルカメラに装着したメモリカードから読み出す点が異なる。

【0077】従来は、ユーザがバスキーを入力できないか、或いはバスキーの入力が困難な端末同士、すなわち

固定バスキーを用いる端末同士が通信開始時に認証処理を行う場合、認証手続きを実行できなかったが、第2の実施形態によれば、どちらか一方の端末(本実施形態においてはデジタルカメラ300)が、通信相手端末のBD__ADDRとバスキー(本実施形態においてはプリンタ400のBD__ADDR__PとバスキーP)を予め外部機器によって書き込んだメモリカードを装着し、認証実行時にメモリカードから読み出して使用することにより、認証処理を行うことができる。従って、セキュリティを確保した状態で接続通信することができるようになるという効果がある。

【0078】また、メモリカードにプリンタ400のBD__ADDR__PとバスキーPを格納してあるため、このメモリカードを別のBluetooth搭載のデジタルカメラ等に装着することにより、当該デジタルカメラ等は、プリンタ400との間で認証処理を実行することができるようになる。

【0079】さらに、通常はキー入力を必要としない機器は、バスキーを入力するためだけに入力手段を持つ必要がないので、コストアップを招くことなく認証処理を実行できるようになるという効果がある。

【0080】なお、第1実施形態及び第2実施形態においては、デジタルカメラ内蔵の2次記憶部112またはデジタルカメラに装着可能なメモリカード314にプリンタのBD__ADDR__PとバスキーPを書き込んでおき、認証実行時に使用したが、これとは逆に、プリンタ内蔵のメモリ不揮発性メモリ204またはプリンタに装着可能なメモリカード413にデジタルカメラのBD__ADDR__DとバスキーDを書き込んでおき、認証実行時にプリンタ内でバスキー検索処理を行い、BD__ADDR__DとバスキーDを読み出して認証処理に使用し、第1実施形態及び第2実施形態において説明したデジタルカメラとプリンタの役割を入れ替えて動作させることも可能である。

【0081】さらに、第1実施形態、第2実施形態では、認証実行時に使用する認証用情報としてBluetoothバスキーを使用していたが、Bluetoothバスキーの代わりに異なる文字列等からなるパスワードを使用しても構わない。Bluetoothバスキーを使用する場合は、ネットワーク階層のリンク層で認証処理を行うが、パスワードを使用する場合は、アプリケーション層で認証処理を行うよう動作する。

【0082】なお、Bluetoothバスキーを使用する場合は、上記のように、ネットワーク階層のリンク層で認証処理を行うので、アプリケーションの開発を効率よく進めることが可能となる。また、認証情報としてパスワードを使用する場合は、上記のように、アプリケーション層で認証処理を行うので、本情報通信システムに対応する情報通信装置を増やすことが可能となる。

【0083】

10

20

30

40

50

【発明の効果】以上説明したように、本発明によれば、通信相手を認証するのに必要な認証情報を入力できない情報通信装置同士でも認証処理を行うことが可能となり、本情報通信システムを利用可能な情報通信装置の種類が増え、利便性が向上する。

【図面の簡単な説明】

【図 1】本発明の第 1 実施形態におけるデジタルカメラの構成を示すブロック図である。

【図 2】本発明の第 1 実施形態におけるプリンタの構成を示すブロック図である。

【図 3】本発明の第 1 実施形態及び第 2 実施形態におけるバスキーリストの一例を示す図である。

【図 4】本発明の第 1 実施形態及び第 2 の実施形態における端末間での認証要求と応答までの処理動作を示す図である。

【図 5】図 4 の処理動作の 1 つであるバスキー検索処理の詳細を示すフローチャートである。

【図 6】本発明の第 1 実施形態及び第 2 実施形態における機器接続リストの一例を示す図である。

【図 7】本発明の第 1 実施形態及び第 2 実施形態における 2 つの端末間での認証要求と応答までの処理動作で、認証役割交換が行われる場合の動作を示す図である。

【図 8】本発明の第 2 実施形態におけるデジタルカメラの構成を示すブロック図である。

【図 9】本発明の第 2 実施形態におけるプリンタの構成を示すブロック図である。

【図 10】従来の 2 つの端末間における認証手続き動作を示す図である。

【図 11】従来の 2 つの端末間における認証手続き動作のうち、認証役割交換が行われる動作を示す図である。

【図 12】従来の 2 つの端末間における認証手続き動作のうち、認証役割交換が行われず、認証手続きが失敗し、終了する動作を示す図である。

10 【符号の説明】

100, 300 : デジタルカメラ本体

101, 201, 301, 401 : CPU

102, 202, 302, 402 : ROM

103, 203, 303, 403 : RAM

104, 204, 304, 404 : 不揮発性メモリ

105, 205, 305, 405 : ワイヤレス通信回路部

107, 207, 307, 407 : 外部機器接続コネクタ

112, 211 : 2 次記憶部

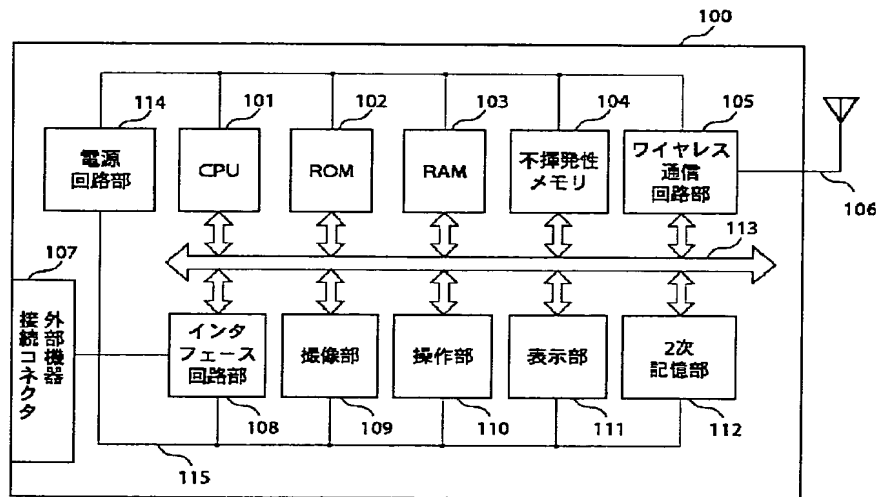
200, 400 : プリンタ

314, 413 : メモリカード

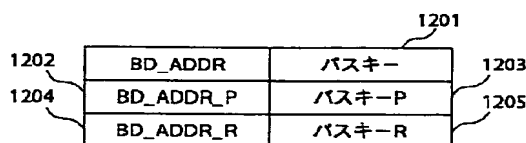
1101 : 機器接続リスト

1201 : バスキーリスト

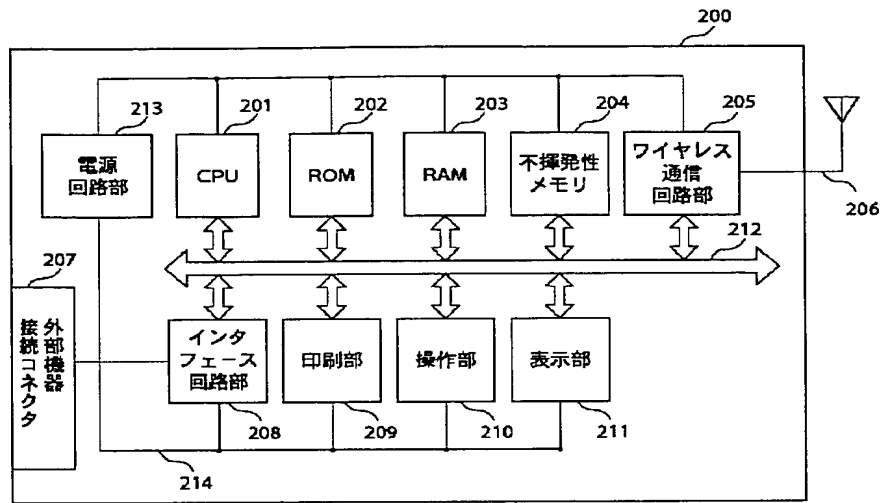
【図 1】



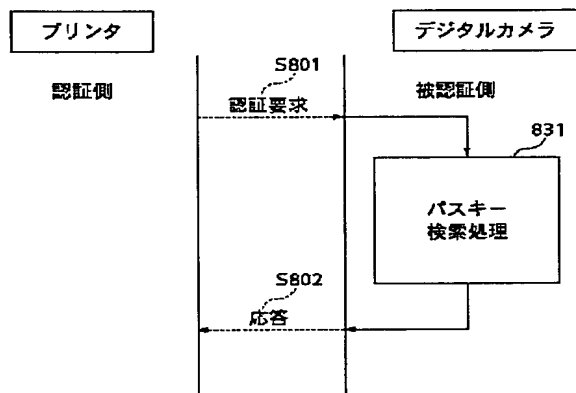
【図 3】



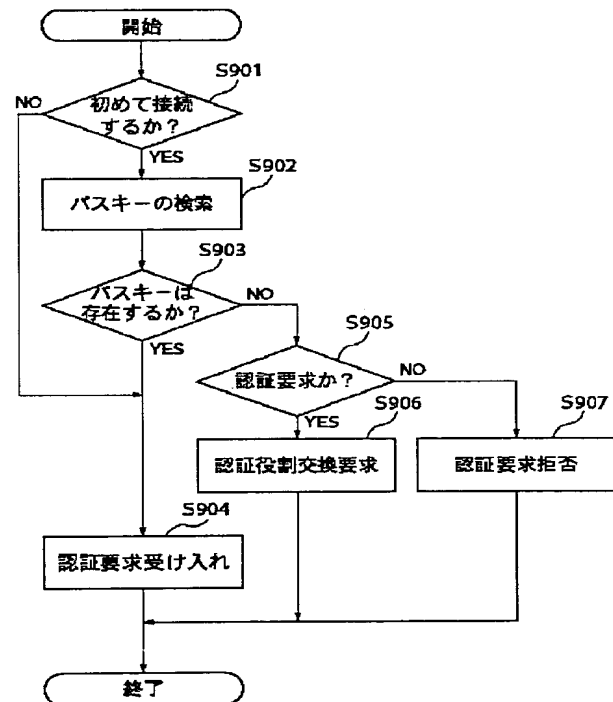
【図2】



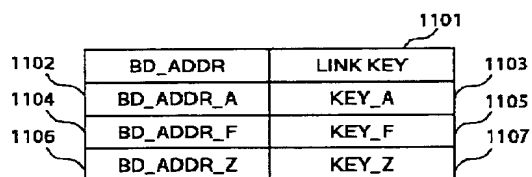
【図4】



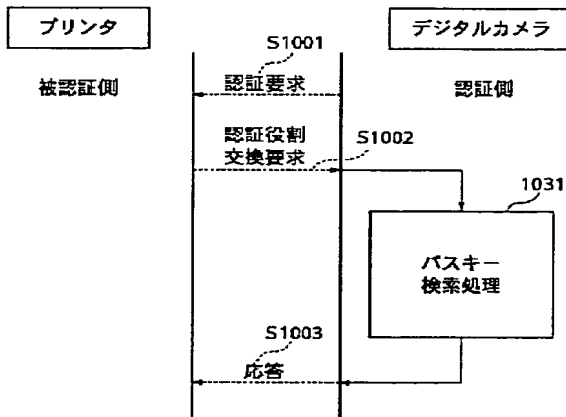
【図5】



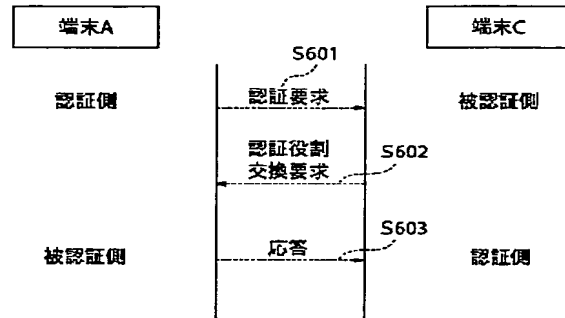
【図6】



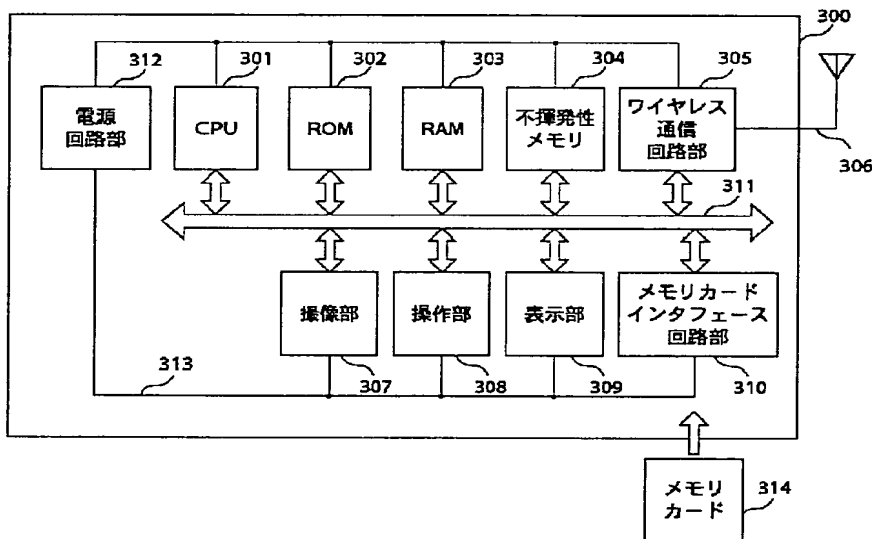
【図7】



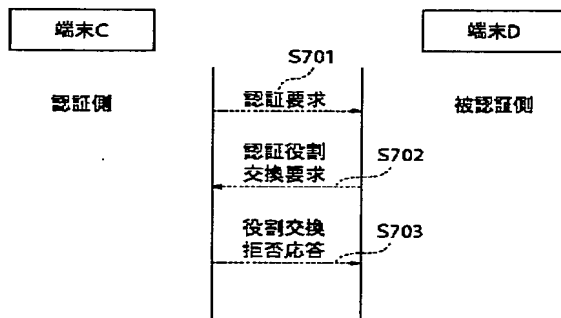
【図11】



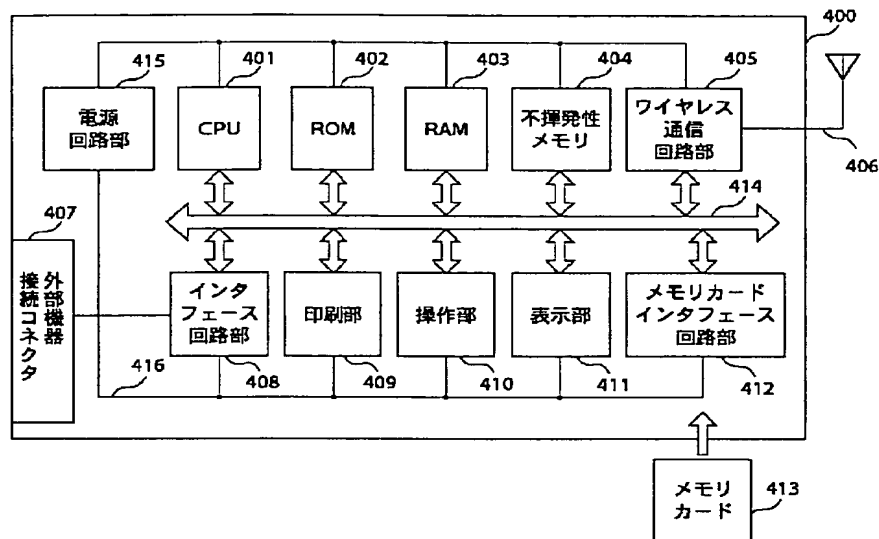
【図8】



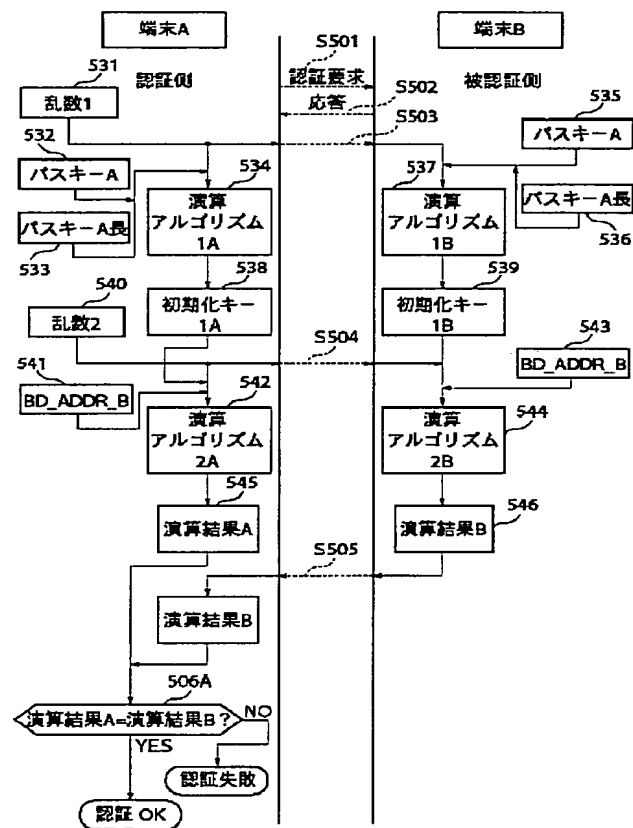
【図12】



【図9】



【図10】



THIS PAGE LEFT BLANK